#17

Legal Affairs Office

Citibank, N.A.
909 Third Avenue
32nd Floor
New York, NY
10043

212/559-0076
Fax
212/793-2516

James A. Button
Vice President and
Senior Technology
Counsel

ENTERED
2/13/97

CITIBANK®

February 12, 1997

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Avenue, N.W.
Room 2705
Washington, D.C. 20230

Re: Encryption Items Transferred to the Commerce Control List

Dear Ms. Crowe:

Citicorp respectfully submits the following comments to the Bureau of Export Administration ("BXA") of the U.S. Department of Commerce ("Commerce") regarding the interim final rule published at 61 F.R. 68572 ("Interim Rule"). The Interim Rule amends the Export Administration Regulations ("EAR") to address licensing and other issues related to the transfer of certain encryption items ("Encryption Items") from the U.S. Munitions List to the Commerce Control List. Our comments first provide background information on the needs of Citibank and other banks and their respective subsidiaries and affiliates (generally referred to throughout this letter as "financial institutions") to use in the conduct of their business robust and trusted encryption that is exportable with minimal administrative burden. We then set out policy level comments on the Interim Rule and policies it embodies. Finally, we provide specific regulatory changes that should be made to the Interim Rule.

Summary

While we view the Interim Rule as potentially a good start in relaxing encryption export controls and applaud the Administration for certain positive steps taken therein, we are deeply concerned that the Interim Rule is not the result of an open, market-driven process. It also fails to codify more favorable treatment for financial institutions' export of cryptography, and falls well short of effectively meeting the needs of financial institutions we outline below. As written, we do not believe the Interim Rule will promote the robust growth of global electronic commerce and secure communications.

Although our comments are detailed and touch on numerous areas of concern, we summarize our primary concerns and recommendations as follows:

- **the Interim Rule must be revised to reinstate the language of the so-called "money or banking" exception previously found in Category XIII(b)(1)(ii) of the ITARs, which has been omitted in ECCN 5A002 of the Interim Rule.** We have been advised that this omission is merely an oversight, but want to ensure that this issue is not lost in the shuffle

because the potential ramifications to financial institutions of losing this important exception are severe;

- the Interim Rule should be revised to relax encryption export controls beyond the money or banking exception for financial applications and financial institutions' systems, with minimal administrative burden and without the imposition of key recovery or key escrow requirements;
- with respect to recoverable and non-recoverable encryption products not limited to financial applications or systems, and key agent requirements, the Interim Rule requires numerous substantive changes if there is to be meaningful buy-in from business and users such that a truly workable and accepted recovery infrastructure may become reality;
- the Administration should use the Interim Rule as an opportunity to clarify uncertainties in the areas of proprietary software that qualifies for mass market treatment, satisfying affirmative acknowledgment, written assurance and similar requirements, and the personal use exemption; and
- the Administration should revisit its decisions to exclude the applicability of the publicly available exception, foreign availability analysis and de minimis rules to Encryption Items.

Background

Citicorp and its subsidiaries ("Citicorp") is a highly diversified, global financial services institution serving the banking, credit card, investment and other financial needs of individual, corporate and government customers in 98 countries. We conduct business through a variety of media and engage in various activities in concert with foreign branches, subsidiaries, affiliates and third parties. Secure electronic communication, both with our customers and internally within our institution, is absolutely essential to our ability to compete in today's international marketplace. Citicorp and other financial institutions must be able to communicate securely with their customers, subsidiaries, affiliates and others on a real-time basis -- and vice versa -- with mutual assurance of the authenticity, integrity, non-repudiation and privacy of those communications. The cornerstone of Citicorp's relationship with its customers is trust - it is axiomatic that a customer and others will not do business with a financial institution they do not trust to protect the security of their information. Providing such security is both good, sound business practice and necessary to deter electronic bank fraud and other illegal activity. In the face of more aggressive and sophisticated technology that can be used to intercept or alter communications transmission, financial institutions must be able to readily export and implement robust encryption products to safeguard the transactions and information on computer networks for themselves and for their customers, affiliates, subsidiaries, partners, and suppliers who increasingly have access to their networks. Exportable, robust cryptography that is widely trusted to ensure authenticity and integrity and to protect confidentiality is an absolutely essential and critical component of this trust relationship.

Citicorp has a long history of involvement and support in the commercial encryption area, both directly and through its affiliation with the American Bankers Association ("ABA"), the U.S. Council for International Business ("USCIB"), and other industry groups. Citicorp has for many year supported and used the Data Encryption Standard ("DES") to secure financial transaction and other financial business-related communications with its customers, affiliates and subsidiaries. With significant amounts invested in DES encryption products around the world, we continue to strongly support DES and private sector control of that standard and continue to strongly advocate that export controls be immediately, permanently and unconditionally lifted from any hardware or software product that uses the DES algorithm or any algorithm that

replaces DES, without any restriction on key length and without any requirement for a key escrow or key recovery process. This is at the core of ongoing legislative efforts to relax export controls on robust, commercially-available encryption products and is consistent with the recommendations of the National Research Council Study ("NRC Study").

The most promising marketplace of today and the future is the Global Information Infrastructure. A secure and trusted Global Information Infrastructure is essential to promote economic growth and to meet the needs of delivering services to our customers in this marketplace. Today, more than ever before, business requires increasingly sophisticated electronic communication -- by computer network, fax, telephone, video, cellular and wireless transmissions, etc. -- and the corresponding freedom to use both proprietary and commercially available robust encryption products worldwide. Financial institutions need to use or allow the use of on-line credit or cash transactions, personal home banking, and other novel on-line services to effectively compete today. Our customers demand and require privacy protection to use global networks for financial transactions. To meet these demands and requirements, we must be free to use both proprietary and commercially available, robust encryption products to be certain of with whom we are dealing, that transactions will neither be tampered with nor repudiated, and that privacy of transaction information is preserved.

In developing export control policy, the Administration must recognize that promoting the development of global electronic commerce to its fullest potential requires strong, flexible, internationally trusted and widely-available cryptography. To be effective, cryptography export control policy and regulations effectuating such policy must be based on the following criteria: (1) voluntary, market-driven development of encryption technology and the products implementing the technology; (2) public availability and evaluation of the technology prior to general commercial use; (3) freedom of user choice by providing for varying degrees of strength to meet requirements for both applications requiring high security (e.g. large dollar funds transfers) and those for lower dollar transactions (e.g. ATMs and credit cards); (4) availability in both hardware and software products; (5) general exportability to end-users without prior governmental approval or unreasonable administrative burden; and (6) broad international acceptance.

It must be made clear that financial institutions require immediate, substantive relaxation of encryption export controls, without imposition of key recovery or key escrow requirements. This is true even though financial institutions already receive more favorable treatment than other industries in exporting encryption products. Outside of favorable licensing policies for financial transaction communications and the current "money or banking" exception for financial applications previously found in Category XIII(b)(1)(ii) of the ITARs and ECCN 5D002 of the EAR (the "money or banking exception"), **which we again reiterate must be restored in the Interim Rule,** financial institutions generally face the same uncertainty regarding exportability of robust encryption products and the same inefficient licensing process as do all would-be exporters. We have fully supported the ABA's, USCIB's, the National Research Council's and others' ongoing recommendation that the U.S. Administration work with the private sector and Congress in an OPEN forum to develop a comprehensive policy on the commercial use of cryptography and we look forward to being an active participant in future developments.

Our remaining comments are set forth in two parts. We first provide a series of general, policy level comments and considerations regarding the Interim Rule which form the basis for many of

our specific comments and suggested changes to various parts of the Interim Rule, which follow our policy level comments.

Policy Level Comments

Our policy level comments touch on the following areas: (1) the need to correct an apparent oversight regarding "money or banking" encryption products; (2) the immediate needs of financial institutions for more relaxed controls on robust cryptography products without key recovery or key escrow requirements; (3) issues and licensing policies raised by the Interim Rule relating to key recovery products, and to non-key recovery products utilizing 56 bit DES or equivalent strength encryption; (4) key recovery product and key recovery agent criteria and standards; (5) "mass-market" qualification for proprietary company products; (6) satisfying "affirmative acknowledgment" and "written assurance" requirements; and (7) issues related to the publicly available exception to the EAR, foreign availability considerations, and de minimis rules.

1. Need to Correct an Apparent Oversight Regarding the Money or Banking Exception.

The Interim Rule omits the "encryption of interbanking transactions" as an exception to encryption license requirements under paragraph h. to the note at the end of ECCN 5A002. Paragraph h. must, at a minimum, be revised to track the language of the "money or banking" exception previously found in Category XIII(b)(1)(ii) of the ITARs and old ECCN 5D13A (which as of January 1, 1997 became ECCN 5D002). We have been informed that the omission in paragraph h. is simply an oversight. The language of this important exception **must** be preserved. Under the money or banking exception, many financial hardware products and software applications automatically transferred to BXA without the need for a CJ request. Retraction of this exemption through the Interim Rule would result in the significant loss of export privileges for financial institutions without a fair opportunity to weigh in on the issue. Moreover, removing the exemption will create severe hardship on financial institutions in terms of rolling out new applications and maintaining and updating their existing base of applications. Financial institutions simply cannot afford to lose this exemption. We also point out that licensing policies in both the State Department and Commerce have been relatively liberal for financial transaction encryption products for the reasons set forth in Policy Level Comment No. 2. below, and we expect that will continue to be the case. We propose specific wording changes below.

We commend BXA for effectuating the move of money or banking applications to ECCN 5D995 and the consequent exportability under license exception TSU. This is a significant change that we have been requesting for some time to remove both the unnecessary written assurance requirement and the anomaly that was created in 1994 between GTDR/TSR (which requires written assurance for western countries) and GLX/CIV (which does not for formerly controlled eastern bloc and other countries).

2. More Robust Encryption Products For Financial Applications and Financial Systems without Government Imposed Key Recovery or Key Escrow Requirements

It is extremely important that the Interim Rule further relax encryption export controls for financial institutions beyond the current money or banking exception without the

imposition of key recovery or key escrow requirements. The Administration has supported, and proclaimed its intention to continue and even improve upon, the historically favorable treatment accorded the export of robust encryption products by financial institutions. Financial institutions have an immediate need for robust encryption products that are exportable with minimal administrative burden, both to provide financial services to customers and to secure their own computer systems and communications networks. Key recovery and key escrow are simply not necessary and do not make sense for financial institutions.

a. The Interim Rule should Codify more Liberal Treatment of Exports of Robust Encryption Products by Financial Institutions. As the government has long recognized, there are strong national and economic security reasons to allow financial institutions to readily export strong encryption products. The Interim Rule should be used to codify the government's commitment to ensuring a highly secure financial system with minimal burden on financial institutions.

b. Strict Cryptography Controls are not Required for Financial Institutions. As the government has also long recognized, highly secure communications between or within financial institutions and between financial institutions and their customers simply do not raise the national security and law enforcement issues that underlie the government's stated desires for strict cryptography export controls. Moreover, financial institutions are highly capable of ensuring that appropriate safeguards are in place to prevent the unauthorized or unintended use of cryptography. Financial institutions can (and do) design their products to ensure that cryptography is not user-apparent and that it can be used solely for purposes of conducting business with the financial institution (e.g. the cryptography can only be used when communicating with the financial institution regarding financial services and related matters). Financial institutions also typically screen their customers through a comprehensive "know your customer" process to help ensure only legitimate end-users can avail themselves of their services and technology. Financial institutions enter into written contracts with their customers which restrict the authorized use of the technology to dealing with the institution (and which also obviates the need for redundant and highly useless written assurances).

c. Key Recovery and Key Escrow Should Not be Imposed on Financial Institutions. Key recovery and/or key escrow should not be mandated for financial institutions' export and use of robust encryption products because such requirements are simply not necessary or desirable. Financial institutions do not take any action on the basis of encrypted data in the form in which it is received in real-time communication and do not generally store data in encrypted form. Communications between or within financial institutions and between financial institutions and their customers are generally encrypted only from the time of initial transmission until receipt by the recipient - typically 1-2 seconds. Financial institutions first decrypt and then act upon the data, and then generally store the data in unencrypted form. Therefore, in the unlikely event that government access to such data is necessary, financial institutions are able to make the unencrypted plaintext of data available pursuant to legal process without any need to store or archive keys. Financial institutions have a long, well-established track record of working closely with the government in this regard without direct government access to bank files, computer systems, or encryption keys. No demonstrated need exists to alter this effective relationship to meet national security, law enforcement or any other needs.

Indeed, altering this relationship by imposing key recovery or key escrow requirements on financial institutions, which may undermine customers' trust in the ability of financial institutions to protect their financial information, is counterproductive and potentially harmful to our competitive position.

With respect to financial institutions, therefore, their is no need for either government imposed key recovery or key escrow or for more than the most basic export controls on financial institutions' use of cryptography (such as those provided by license exception Technology and Software Unrestricted (TSU)). The Interim Rule should relax export controls on encryption used in financial applications and to secure financial institutions' systems without restriction on encryption key length or modulus size, and without requiring key recovery or key escrow. Our specific current needs for relaxing encryption export controls for financial institutions are as follows:

i. Financial Applications. We need the immediate freedom to use robust versions of both asymmetric key products such as RSA for authentication, data integrity, verification, non-repudiation, and secure digital signature capability, and symmetric key products such as those that utilize DES, RC4, etc. to encrypt information. Provided that such cryptography is used only in financial products and solely for the purpose of conducting business with a financial institution, and not for encryption of general communications, such products should be automatically exportable to customers under license exception TSU, without written assurance (or similar License Exception if implemented in hardware), regardless of modulus size or key length and without mandated key recovery or key escrow. Immediate action is needed in this area - - financial institutions and customers worldwide are demanding and requiring significant levels of security. Foreign competitors are already providing it and in many cases proliferating it free of export controls.

ii. Financial Information Systems. In a similar vein, financial institutions need the immediate ability to export strong proprietary and commercially-available cryptographic products to their affiliates, subsidiaries and service providers abroad to secure the financial institution's internal computer systems, networks and other internal communication systems. Communications across internal bank systems also do not present national security and law enforcement concerns, but are increasingly vulnerable to sophisticated fraud schemes and intrusive attacks. Asymmetric key products and symmetric key products should be made exportable under license exception TSU (or similar License Exception if implemented in hardware), regardless of modulus size/key length and without mandated key recovery or key escrow, if used solely by financial institutions and their affiliates and subsidiaries to secure their own internal systems.

In our specific comments below, we provide suggested revisions to the Interim Rule to address the above considerations.

If the Administration is not inclined to relax encryption export controls to the extent that Citicorp suggests above, we implore the Administration to provide such additional relief without mandated key recovery or key escrow, subject only to a limit on modulus size/key length that recognizes the extreme importance of security in financial applications and financial institutions' internal systems. Given that the Interim Rule

generally relaxes export controls on 56 bit DES and equivalent strength encryption products that have long been restricted to use by financial institutions, the Interim Rule should, at a minimum, correspondingly relax export controls on encryption products used by financial institutions in their financial applications and to secure their internal systems to the following levels: (i) asymmetric key products such as RSA: 2048 bit modulus size; (ii) DES: triple DES key length; and (iii) RC4 and similar symmetric key products: 128 bit key length. Such an approach would effectively codify meaningful relief for financial institutions to a level of security that meets our needs for the foreseeable future. If such an approach is adopted, exportable modulus size and symmetric key length would need to increase over time to keep pace with the rapid and dynamic changes in technology. BXA, working with the financial services industry, should create automatic, periodic adjustments in key lengths that maintain equivalent levels of information security in the future.

3. Key Recovery Issues and Licensing Policies Raised by the Interim Rule[1]

For the reasons set forth above, key recovery and key escrow requirements should not be imposed on the use and export of robust cryptography by financial institutions. If, however, the Administration refuses to modify the Interim Rule to meet the immediate needs of financial institutions as we propose above and is determined to proceed with the approach of the Interim Rule as written, then it is critical to do it correctly. Citicorp is concerned with various aspects of the Interim Rule as it pertains to "key recovery," "key escrow," a "key management infrastructure," and "other recoverable encryption products." Contrary to the tone of Executive Order 13026, the Interim Rule effectively mandates third-party "key escrow" as the only practical form of "key recovery." This is evident from the Supplementary provisions of the Interim Rule and **Supplement No. 4 to Part 742 - Key Escrow or Key Recovery Products Criteria.** This approach is inconsistent with the fundamental principles of user choice and voluntary, market-driven solutions that the Administration propounds and jeopardizes the chances of meaningful industry and user acceptance. Several substantive changes to the Interim Rule are required if there is to be meaningful buy-in from business and users such that a truly workable and accepted recovery infrastructure may become reality.

3.1 There is no Apparent Demand or Use for Recoverable Products for Communications

As previously indicated, no "key management" system will be successful unless it is voluntary and market-driven, and unless it is practical and makes sense to the business and user community. Users of cryptography will not accept what they do not want or what they do not see as providing value, and business cannot sell what users do not want. Inasmuch as there seems to be some consensus in both the private and public sectors that there may be demand for products that allow for the recovery of stored encrypted data, then as a policy matter, if key recovery is to be mandated in exchange for relaxed encryption export controls, key recovery should be a condition of exportability only with respect to stored data. There is no apparent commercial demand or need for key recovery in real-time communications. There appears to be no evidence that users want

[1] Citicorp's comments in this section and related changes suggested later in this letter should not be interpreted as detracting in any way from our comments and suggested changes in Policy Level Comments Nos. 1 and 2 above.

the ability to recover the plaintext of encrypted data in transit; rather, users only want the ability to recover the plaintext of encrypted data after the communication is completed. If encryption export control policy does not align with users' needs, it will be self-defeating.

Requiring the escrow of keys or key recovery for real-time communications data may not be technically feasible in a practical sense, has been highly criticized by software manufacturers and others, and places significant burdens on the business community to recover and maintain thousands (or millions!) of session keys generated on a daily basis by employees, customers and others. Citicorp and other businesses may choose to, but should not be forced to, absorb the cost of such a scheme, and it does not make sense in any event for the reasons set forth in our Policy Level Comment No. 2 above. Even Commerce's own technical advisors on these issues, the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, has acknowledged the significant difficulties posed by such a requirement. In contrast, technology that provides for recovery of plaintext of stored data is something that software manufacturers have been addressing and appear able and willing to implement in their products to meet customer demand. Key recovery with respect to real-time communications as a condition to exportability should be removed from the Interim Rule.

3.2 Recommendations Regarding Recoverable Encryption Products

The following summarizes our general recommendations regarding key recovery aspects of the Interim Rule.

a. The Interim Rule must focus on "key recovery" and "other recoverable encryption products," not just "key escrow". Simply put, a recoverable encryption product that maintains data confidentiality should be freely exportable, regardless of key length, so long as it allows for the recovery or accessibility of the plain text of that data without the assistance of the party who encrypted the data. There should be no requirement whatsoever that (i) key recovery with respect to real-time communications be implemented, (ii) a copy of any encryption key (whether the key is used for data encryption, authentication, to verify data integrity, or for any other purpose) or the ability to access or reconstruct the key be given to any third party, or (iii) a business must archive keys. We strongly encourage the Administration to re-examine the Interim Rule and to modify any aspect thereof that purports to be "key recovery" or to promote "recoverable" concepts, but in effect implements "key escrow" concepts or requirements, so as to focus the Interim Rule on stored data recovery principles.

b. The key recovery agent requirements set forth in Supplement 5 to the Interim Rule are far too burdensome to companies who choose to maintain their own internal key management infrastructure and are too skewed towards U.S. persons. If Citicorp and other companies choose to implement a key management infrastructure, then they must be free to archive and manage keys themselves, through their own employees and agents worldwide, without regard to nationality (other than nationals of embargoed countries). While we recognize that the Interim Rule does not prevent Citicorp from establishing an internal key management process, it is extremely

important that maximum freedom and flexibility be clearly reflected in the requirements for Key Recovery Agents. We make specific suggestions in this regard below.

c. Licensing Policies. If the Interim Rule is to provide immediate and meaningful relief on encryption export controls in a manner that recognizes business needs and realities of the marketplace, then the following principles should be clearly stated throughout the Interim Rule, and at a minimum in Parts 740.8 and 742.15, and the related Supplements:

   i. Generally, export of commercial encryption products should be permissible under the least restrictive license exception (e.g. TSU), without a written assurance requirement. Specifically, mass market encryption products utilizing 56 bit DES, 128 bit symmetric RC4 and equivalent strength similar symmetric cryptography, and/or 1024 asymmetric RSA and equivalent strength asymmetric cryptography, must be immediately exportable under license exception TSU without any requirement for key recovery or key escrow.
   ii. Recovery products that allow stored data recovery should be exportable under license exception KMI, after meeting objective tests or, for close calls, a one-time BXA review, regardless of the strength of the encryption algorithm used or key generation technology employed.
   iii. No BXA review or key recovery commitments should be required for the continuing export of products already reviewed and transferred to Commerce prior to publication of the Interim Rule.
   iv. No BXA review should be required for any "new" product if the only change in the product is to provide 56 bit DES, 128 bit RC4, 1024 asymmetric, or equivalent strength encryption. BXA should be satisfied with written confirmation of such change from the manufacturer.

d. 56 bit DES and Equivalent Strength Non-Recoverable Products. If the government is not inclined to relax export controls as we previously suggest, then at a minimum the successive six month approval requirements for 56 bit DES and equivalent strength non-recoverable products set out in Parts 740.8(d) and 742.15(b) must be replaced with an automatic two year license. The six month approval process creates far too much government intervention in and micromanagement of business affairs, provides too short a period of time for meaningful relief, creates too much uncertainty, and will likely severely limit both the willingness of U.S. companies to deploy such products and the willingness of overseas companies to use them. The requirements as written place far too much burden on would-be exporters to provide the government with confidential and sensitive business information that is not required to effectuate the intent of the Interim Rule.

   It would be far preferable to simply allow the immediate and unconditional export of 56 bit DES and equivalent strength products for two years and give business the full two years to export and use such products without the bureaucracy and government intervention inherent in the Interim Rule. If after the two year period, stored data recovery requirements are not met, the license exception for such products can be removed or modified. As a further alternative, BXA could require reports at six month intervals and reserve the right to revoke the license if satisfactory progress

towards recovery is not demonstrated in such reports. Such an approach provides more meaningful export control relief and would incent business to build and deploy recovery products.

e. Interoperability. The Interim Rule does not address interoperability considerations very well. We believe, again, such issues are best left to the marketplace. More specific comments on this issue are provided below.

4. Key Recovery Product Criteria and Key Recovery Agent Standards

The Interim Rule sets out bureaucratic, unworkable and self-defeating criteria and standards that are almost exactly the same criteria that NIST unveiled in 1995 and that industry has consistently rejected. Few of industry's concerns have been addressed. Again, the criteria and standards here should be based on voluntary, market-driven, and user-choice principles. The Administration should revisit both of these areas in a serious attempt to establish simpler, self-executing requirements that rely on industry expertise and compliance. For a variety of reasons, Citicorp does not see how a workable, world-wide key recovery process will be established under the current requirements of the Interim Rule. We believe that most multi-national companies will reach the same conclusion. Therefore, these standards and criteria are counterproductive and self-defeating. More specific comments and recommendations are included below.

5. "Mass-Market" Qualification for Proprietary Company Products

An extremely important issue to a financial institution is when, and under what circumstances, its own proprietary software products that are generally distributed to customers may qualify as "mass-market" software under the General Software Note (GSN) of the EAR. Historically, some BXA officials have taken a rather restrictive view in this area that we believe is unrealistic, unjustified and harmful to Citicorp's and other companies competitive position globally. The Interim Rule is an appropriate opportunity to clarify that company proprietary software is eligible for mass-market treatment under the GSN as long as it is (i) made generally available to customers by means of over-the counter, mail order, telephone call, Internet transactions, and/or other forms of general distribution, and (ii) designed for installation by the user without substantial support by the supplier. With respect to (i), it is extremely important that the EAR make clear that company proprietary software is eligible for GSN treatment even if an individual or company must first have a customer relationship with the supplier in order to obtain or make productive use of the software, such as is the case with home banking and other banking software products. Some BXA officials have taken the position that a requirement that a user first be a Citibank customer, which we welcome on a non-discriminatory basis, means that the software is not "sold...without restriction" and therefore cannot qualify under the GSN. We believe this position draws a distinction with no meaningful difference. In the U.S., we give away user-installable home banking and other software to customers through mass market channels, so being a customer is no more of a "restriction" than paying an over-the-counter license fee in Egghead Software. Further, as previously noted, particularly in a banking relationship, requiring a prior customer relationship actually helps to ensure that only legitimate end-users receive the software and therefore, as a policy matter, should not serve to disqualify the software from GSN treatment.

6. Satisfying "Affirmative Acknowledgment" and Written Assurance Requirements

BXA should also use the Interim Rule as an opportunity to clarify what it considers to be acceptable means of satisfying the "writing" and "signature" aspects of the new "affirmative acknowledgment" requirements included in Part 734.2(b)(9) of the Interim Rule, as well as for written assurances. This is another area in which BXA has been fairly rigid in the past and out of step with business reality. Notwithstanding the transfer of financial applications software to ECCN 5D995 discussed above, this is extremely important as (i) software and technology distribution increasingly takes place through the Internet and other electronic means, (ii) business tends to err on the safe side in deciding whether written assurance requirements may apply, and (iii) business struggles to define the simplest and most effective ways to meet these requirements. The Interim Rule should be modified to make clear that such requirements may be met in any manner that establishes a legally binding obligation. Any method sufficient to create a legally binding obligation, whether by written signature, electronic means or otherwise, should suffice - there is no reason for BXA to micromanage methods of meeting such requirements in the modern marketplace. Such an approach builds greater certainty today, and allows the flexibility to recognize solutions of tomorrow. As an example of recent developments in this area, BXA should consult (1) the Federal Reserve Board's recent amendments to Regulation E, which provide that electronic banking (via PC, smartphone or other remote device) can satisfy Regulation E "writing" requirements if required notices are displayed on screen and if a hard copy of transactions and balances are made available upon request; and (2) the various state Digital Signature laws, which provide that a defined "electronic signature" may be used to sign a writing and shall have the same force and effect as a written signature.

7. The Publicly Available Exception , Foreign Availability and de minimis Considerations

We question the wisdom and practicality of limiting the applicability of these fundamental considerations to Encryption Items. It simply is not a meaningful distinction to claim that export controls on encryption software are distinguishable from controls on other EAR controlled software because of its functional capacity to encrypt information on a computer system, as opposed to any information or theoretical value the software may contain or impart to others. All software controlled on the CCL is controlled based on functionality, not its information content. Excluding Encryption Items from the publicly available exception to export controls under the EAR goes even further than was the case under the ITARs and is unlikely to pass constitutional muster (a la the Bernstein and Karn cases). Removing to a large extent the applicability of foreign availability considerations undermines a key concept in export controls. The reason stated in Part 5 of the Supplementary provisions of the Interim Rule for doing so, which is quoted from section 1(a) of Executive Order 13026, is absolutely unpersuasive. National security interests are not jeopardized by foreign availability considerations because the President has the authority to waive mandatory decontrol of national security controls after a finding of foreign availability. The only purpose this exclusion serves is to cut off critical evaluation as to whether comparable foreign products exist in quantities that render U.S. export controls ineffective in achieving their stated purpose. This exclusion is also fundamentally at odds with a key conclusion of the NRC Study; the reality is that strong encryption products are already available overseas and this trend

will continue. Finally, excluding the application of the de minimis principles to Encryption Items also undermines a key concept and the credibility of export controls for little or no apparent benefit. We strongly encourage BXA to reconsider its position on all of these issues and allow Encryption Items to be subject to all the provisions of the EAR.

Specific Regulatory Change Comments

Citicorp submits the following specific comments and recommendations regarding the provisions of the Interim Rule. These comments are presented in the order in which they appear in the Interim Rule and not in any order of importance or precedence. All references are to the noted page number of the Federal Register at Vol. 61, No. 251. To the extent you would like further drafting suggestions or clarifications on our proposed changes to the Interim Rule, please feel free to contact me at the phone number listed at the end of this letter.

A. Summary; Supplementary Information

1. The last sentence of subpart *(2) Key Escrow, Key Recovery, and Recoverable encryption software and commodities,* on page 68574, which reads in part "...the plaintext of the encrypted data and communications will also receive..." (emphasis added) is the first instance where the **plaintext of encrypted communications** is referenced. In keeping with our Policy Level Comment No. 3, this and all other references to "communications" should be deleted. Conforming deletions would then need to be made to all other references to "communications" in such context throughout the Interim Rule (see, e.g., Subpart *(5), Applications for encryption technology* on page 68575 in the definition of "recovery encryption products"; and Parts 740.8(d)(ii) on page 68579 and 742.15(b)(2), last sentence on page 68581).

2. W recognize and applaud that License Exceptions TMP and BAG effectively replace the State Department's personal use exemption without the recordkeeping requirements imposed thereby. However, as explained in more detail in our suggested changes below, BXA needs to clarify the application of the exemption in Parts 740.4 and 740.9, as well as in ECCN 5D002 to ensure that the exceptions apply to Group D countries, to exhibition and demonstration in all but Group E:2 countries, and to License Exception KMI.

3. The definition of "recovery encryption products" set out on page 68575 should be modified to delete the reference to "and communications" and should be moved to, or restated at, Part 772 - Definition of Terms.

4. After the definition of "recovery encryption products" on page 68575 referenced in point 6. above, the Interim Rule states that "(o)ther approaches to access and recovery may be defined in the future." Citicorp would very much like to see a stronger statement added to Part 740.8 to the effect that BXA is committed to work with industry in an open forum to develop alternative, voluntary and market-driven approaches to develop recoverable Encryption Items and a recovery infrastructure.

5. The Administration should reconsider its position on the change to Part 734.2(b)(9)(ii) regarding export of encryption source code and object code software through electronic

download or other transfers. This should be deleted or, at a minimum, changed to a BXA advisory as Citicorp suggests below. If this Part is not deleted, then BXA must, somewhere in the Supplementary part, describe and summarize that change. It is unfair and unwise to simply publish the change as an amendment to the EAR without a discussion of the change in the Supplementary provisions.

B. Comments on Actual Changes to the EAR

1. Delete the amendments to Parts 732.2(b) and (d) and 732.3(e)(2) regarding inapplicability of the publicly available and de minimis provisions of the EAR.

2. Delete all of Part 734.2(b)(2) and (b)(9)(ii). This is a completely new, unexpected and commercially unreasonable requirement that will be routinely and regularly violated.

3. If BXA does not delete all of Part 734.2(b)(2) and (b)(9)(ii), then at a minimum:

- Provide a summary of the new requirement in the Supplementary provisions;
- Change the standard of strict liability in Part 734.2(b)(9)(ii)(B) such that, depending on all the facts and circumstances surrounding particular behavior, the activities enumerated in Part 734.2(b)(9)(ii) might be considered to further an illegal export. It is unreasonable to impose strict liability in the context of posting to the Internet and otherwise "making available" electronic transfers, which will clearly have the effect of criminalizing everyday behavior not currently considered by most people to be illegal (or even wrong!). The ITARs did not regulate this activity - some companies simply sought advisories from the Office of Defense Trade Controls. BXA should structure Part 734.2(b)(9)(ii) as a BXA advisory and establish the precautions set out in Part 734.2(b)(9)(ii)(A)(1)-(3) as "safe harbors." This removes the inequity of criminalizing common behavior and should accomplish the same result from a compliance perspective; and
- delete the following from Part 734.2(b)(9)(ii)(B): ", approved in writing by the Bureau of Export Administration," so that part 734.2(b)(9)(ii)(B) reads: "Taking other precautions to prevent transfer of such software outside the U.S. without a license." If BXA insists on retaining the requirements set out in Part 734.2(b)(9)(ii)(A), even as safe harbors, then at least recognize that business is fully capable of devising, without BXA's involvement or prior approval, the most commercially reasonable and workable alternatives to accomplish the objectives of 734.2(b)(9)(ii)(A)(1)-(3). Exporters who have questions can always apply to BXA for advisory opinions.

Part 734.2(b) is a logical place to clarify BXA's position on exporters satisfying "affirmative acknowledgment" and "written assurance" requirements, as suggested in our Policy Level Comment No. 6. We request that BXA clarify here that any action sufficient to create a legally binding obligation meets these requirements. BXA should also provide such clarification in Part 740.3(d), Technology and Software under Restriction (TSR), and then cross-reference Part 740.3(d) in Part 734.2(b).

4. Delete all changes to Parts 734.3(b)(3), 734.4(b)(2), 734.4(h), 734.7(c), 734.8(a), 734.9, **Supplement No. 1 to Part 734 - Questions and Answers - Technology and Software**

Subject to the EAR, and Part 772 (definition of "Commodity"), as they pertain to limiting or excluding the applicability of the public availability and de minimis provisions of the EAR to Encryption Items.

5. If BXA is not inclined to make the changes suggested in 1. and 4. above, then at a minimum clarify the various Parts of 734 and Supplement No. 1 to Part 734 enumerated in 1. and 4. above, as well as applicable provisions of Parts 740.8, 740.13(d)(2) and 742.15(a), to make clear that software and technology that was subject to the EAR as it was in effect as of the publication date of the Interim Rule is not subject to these various Encryption Items controls set forth in the Interim Rule. While we acknowledge that the statements made in ECCN 5A002, 5D002 and 5E002 help to address this issue, these statements should also appear in the body of the EAR to ensure that the EAR reflect the clear intent of the Interim Rule (as stated more clearly in the current Supplementary provisions) that all such software and technology continues to be eligible for publicly available treatment, de minimis rule applicability, and the General Software Note, as applicable.

6. Re-write Part 740.8(d)(2) to provide immediate and unconditional relaxation of export controls on 56 bit DES and equivalent strength encryption products, as previously suggested in our Policy Level Comment No. 3.2.c. At a minimum, this Part must be rewritten as suggested in our Policy Level Comment No. 3.2.d. to provide for the immediate relaxation of export controls on such items for a full 2 year period, subject to revocation by BXA for cause at the end of the 2 year period, (or, as an alternative, every six months if satisfactory progress reports are not submitted) and the deletion of all requirements and other provisions related to submitting business and marketing plans, etc. Conforming deletions and changes would then need to be made to all other references to the 56 bit licensing scheme proposed by the Interim Rule (see, e.g., Part 742.15(b)(3) and Supplement No. 7 to Part 742).

7. Delete "and communications" from Part 740.8(d)(ii) on page 68579.

8. Delete Part 740.8(e), which requires semiannual reports of all exports under License Exception KMI. This requirement is extremely onerous to businesses. Further, the need for such requirements, as well as the value thereof to BXA, is highly questionable. As applied to mass-market software, the requirements are extremely objectionable as they are completely inconsistent with mass-market distribution and will be very difficult to comply with. The requirements may therefore defeat much of the potential benefit of mass market distribution of such products. In any event, and particularly with respect to the other provisions of Part 740.8, BXA has the authority to demand the production of export records which satisfies BXA's needs in this regard.

9. Include in Part 740.8 the statements from the Supplementary provisions that after December 31, 1998, exporters will be allowed to service customers who have 56-bit non-recoverable products, as well as to export additional products. These statements, which can be found on page 68574, will be extremely important to potential customers of such products who will want to know, prior to purchase, that their products will be supported after 12/31/98 and should therefore be incorporated into the EAR as law.

10. Add a statement to Part 740.8 to the effect that BXA is committed to working with industry in an open forum to develop alternative, voluntary and market-driven approaches to develop recoverable Encryption Items and a recovery infrastructure.

11. BXA should use the Interim Rule as an opportunity to clarify both Parts 740.4(a)(2)(i) and 740.9(d) of the EAR to correct two lingering minor issues with License Exceptions TMP and BAG. First, Parts 740.4(a)(2)(i) and 740.9(d) should be revised to remove any restrictions on using these License Exceptions for Country Group D. Second, both TMP (at 740.4(a)(2)(iii)) and BAG should be clarified to allow exhibition and demonstration in all Country Groups other than E:2. These changes help to ensure that ordinary, everyday behavior by legitimate business people is not criminalized and bring these License Exceptions more in line with the personal use exemption they replace.

12. Part 742.15(b)(1) is a logical place to clarify the eligibility of company-proprietary software for mass-market treatment, in accordance with our suggestions set forth in our Policy Level Comment No. 5 above. Company proprietary products that are designed for installation by the user without substantial assistance from the supplier and which are made generally available to customers through telephone, over-the-counter, mail-order, and Internet transactions, or other forms of general distribution, should qualify for mass market treatment under the GSN.

13. Part 742.15(b)(3) needs to be rewritten to delete the 6 month license scheme, submission of business and marketing plans and related requirements, as stated in our Policy Level Comment 2 and our Specific Comment B.6 above.

14. Delete "and communications" from the last sentence of Part 742.15(b)(2) on page 68581.

15. **Supplement No. 4 to Part 742 - Key Escrow or Key Recovery Products Criteria.**

These criteria need to be revised as they are limited to key escrow, not key recovery. Our specific suggestions:

Key Recovery Features

- make clear that these "feature" criteria pertain only to recovery of stored data, as opposed to keys, and that the product shall be designed to provide for recovery of plaintext of stored data.
- delete the phrase, "or other material/ information required to decrypt cyphertext", which is found throughout the criteria.

Interoperability

- criteria (6) must be modified to provide that recovery products may interoperate with non-recovery products. Not allowing for interoperability will create significant failures both here and abroad as non-recovery products may be freely used in the U.S., and for at least a 2 year period will remain eligible for export.

Design, Implementation and Operational Assurance

- Criteria (7) should be revised to read: "The product shall be designed to resist efforts to disable or circumvent...six." As written, the criteria sounds like a manufacturer must guarantee resistance, which is not possible.
- Criteria (8) is mandatory key escrow and is not acceptable or advisable for the reasons set forth in our Policy Level Comment No. 3. This criteria should be deleted or stated as an option for companies like Citicorp who may or may not choose to establish a comprehensive key management infrastructure.

16. **Supplement No. 5 to Part 742 - Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures.**

As a general matter and as stated in our Policy Level Comment No. 3, this Supplement is a classic example of overreaching, heavy-handed and unnecessarily intrusive government regulation of matters best left to market forces. Industry knows best how to select and qualify individuals/entities that would act in a key recovery agent role, how to implement safeguards and procedures that ensure a secure environment, and how best to implement key recovery procedures, if such a decision is voluntarily made for business reasons. Similarly, reputable companies will voluntarily establish satisfactory recovery agent services in response to market demand for such services. It simply is not appropriate for government to attempt to set such bureaucratic and strict standards for industry. We are also very concerned with the potential implications of making manufacturers liable for the actions of key recovery agents.

A far preferable approach to Supplement No. 5, and one that is consistent with export controls in general, is for BXA to re-write the entire Supplement to provide simple, straightforward, high-level and self-executing requirements that leave the details of the "how" where it belongs - industry expertise. BXA can rely on enforcement mechanisms as it does in other contexts to ensure industry compliance.

If the Administration is unwilling to change the overreaching and bureaucratic approach set out in Supplement No. 5, then at a minimum make the following changes:

- Revise the Supplement to distinguish clearly between third party agents and requirements and company internal agents and requirements. Focus the entire Supplement on requirements for third party agents.
- With respect to company internal agents, simply state that a company may establish an internal key management infrastructure that (i) provides for a secure, trustworthy process to ensure that the plaintext of stored encrypted data is available to government pursuant to legal process, and (ii) allows for U.S. and non-U.S. citizen employees and third parties under contract with the company to act as internal recovery agents. Leave the remainder of implementation details to business to effectuate such an infrastructure in accordance with its own qualification, security and other policies.
- There should be no right whatsoever for BXA to approve or disapprove a company's internal key management infrastructure. BXA's check on the process should be solely through audit and enforcement mechanisms.

- The Interim Rule needs to address more clearly issues of bilateral and multilateral agreements, and legal standards that will apply to jurisdiction/access outside the U.S.

Key Recovery Agent Requirements

- These requirements are skewed too heavily towards U.S. citizens/persons. The requirements should be broadened to more clearly allow for non-U.S. citizen employee and third party agents.
- The requirements demand too much in terms of what manufacturers/exporters must know about individual customers prior to selling them products, requiring a distinct distribution channel(s) for recovery products.
- Requirement (1)(b)(i)(A) - BXA should review this requirement and consider focusing it on convictions for crimes of dishonesty, such as is the case for bank employees under FIRREA, or perhaps limiting it to convictions for felonies.
- Requirement (4) is simply not workable and could create severe hardship for business. BXA must, at a minimum, provide a grace or transition period during which such compliance can be demonstrated.
- Requirement (8) should be revised and restated in line with the comments above regarding internal agents.

Security Policies

- Again, these requirements are over-reaching and should not, in any event, be mandatory for companies who choose to establish an internal key management infrastructure.

Key Recovery Procedures

- Again, these requirements should not be mandatory for companies who choose to establish an internal key management infrastructure.
- The 2 hour requirement in (1) is unreasonable and there appears to be no valid reason for such a short response time. This is particularly so when the information required to be submitted is taken into account.
- Requirement (3) should be clarified to the greatest extent possible to minimize the effect on business and innocent users of loss of "acceptable" key recovery agent status. This provision should be clarified to require that the transfer shall be designed to occur, to the greatest possible extent, without interrupting users operations, access, etc.

17. **Supplement No. 7 to Part 742 - Review Criteria for Exporter Key Escrow or Key Recovery Development Plans.**

As stated in our previous comments regarding 56 bit DES and equivalent strength products, this Supplement is unnecessary and should be deleted in its entirety.

18. The revisions to Part 768.1, making Encryption Items ineligible for foreign availability considerations, should be deleted.

19. Part 772. Insert the definition of "recovery encryption products" from page 68575 (absent a reference to "and communications") and definitions of "key escrow" and "key recovery".

20. Part 774, Category 5, Telecommunications and Information Security.

- For the reasons set forth in our Policy Level comment 4 above, Paragraph h. to the Note at the end of ECCN 5A002 should be deleted in its entirety and replaced with the following to restore the money or banking exception and to clarify the past practices of the ODTC with respect thereto:

  "h. Cryptographic equipment specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include but are not limited to automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions."

  At a minimum, BXA should replace the language at paragraph h. with the language previously found in Category XIII(b)(1)(ii) of the ITARs and the Advisory Notes to old ECCNs 5D13A and 5D002.

- A new paragraph i. should be added to the Note at the end of ECCN 5A002, as follows:

  "i. Cryptographic equipment specially designed, developed or modified for use in conducting financial transactions between a financial institution and its customers, provided that such equipment can be used solely to conduct business with a financial institution and for no other purpose."

  Alternatively, the language proposed as new paragraph "i" could be incorporated into paragraph h.

- A new paragraph j. should be added to the Note at the end of ECCN 5A002, as follows:

  "j. Any cryptographic equipment that is used by a financial institution solely for the purposes of securing its own internal computer systems, networks and other information processing and communications systems and for no other purpose."

- If the Administration does not agree with the above suggested new paragraphs i. and j. as proposed, then alternatively add the new paragraphs i. and j., with (1) limits on encryption algorithm strength of triple DES for products that use DES, 128 bit key length for RC4 and other equivalent strength symmetric key products, and 2048 bit modulus size for asymmetric key products, and (2) a process for automatically increasing key bit length and modulus size in the future.

- ECCN 5D002 should be clarified to make clear that License Exceptions TMP and BAG apply to License Exception KMI. We propose that the last sentence in the first

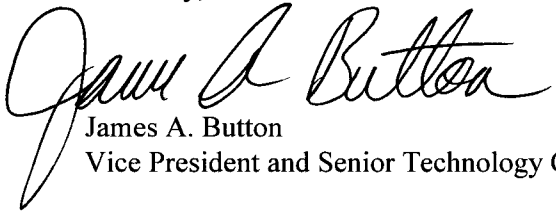
paragraph of the note the ECCN 5D002 be revised to read: "License Exceptions other than TMP and BAG, are not applicable for commodities."

21. **Supplement No. 2 to Part 774 - General Technology and Software Notes.**

The General Software Note is another logical place that BXA could clarify the eligibility of company proprietary software for Mass-market treatment in accordance with our Policy Level Comment No. 5.

We appreciate this opportunity to comment on the Interim Rule and look forward to working with the Administration in the future on encryption export control policy. If you wish to further discuss any of the above matters, please feel free to contact me directly on (212) 559-0076.

Sincerely,



James A. Button
Vice President and Senior Technology Counsel

cc: Mr. David Aaron
Mr. Edward Appel
The Honorable Robert Bennett
The Honorable Conrad Burns
Mr. John Byrne, ABA
The Honorable Michael Castle
Mr. Abraham Katz, USCIB
Mr. James Lewis
Mr. Ira Magaziner
Mr. Vito Potenza